MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2015/2016

TMI 3231 - MALWARE AND INTRUSION DETECTION

(All sections / Groups)

1 MARCH 2016
2:30 p.m – 4:30 p.m
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 7 pages with 6 Questions only.
2. Attempt **FIVE** out of **SIX** questions. All questions carry equal marks and the distribution of the marks for each question is given.
3. Please print all your answers in the Answer Booklet provided.

QUESTION 1

a) As a security professional in an e-commerce company, you are to ensure that your company is making the right decisions in protecting its web servers and information. Your company is faced with two extreme measures that are proposed by two general managers of the company. State your opinion about each of the proposals and support your opinion with appropriate justifications.

Proposal A: The company should highly protect its web servers to ensure that it cannot be attacked. Therefore, the company needs to place its servers within the internal network and closely regulate and restrict access to the server.

Proposal B: In order to gain more customers and encourage connectivity, the focus should be more on accessibility. Therefore, traffic to servers should not be regulated or monitored since it could highly slow down our connectivity and speed.

(4 marks)

b) Session hijacking is an attack in which a legitimate user session is hijacked. Explain how such attacks are performed.

(2 marks)

c) You are analyzing a new system that your company is going to use very soon and you found that the new system does not enforce proper input validation and representation mechanisms. You would like to report this incident to your top manager. State and explain FOUR (4) attacks/issues that could arise as a result of having poor input validation and representation mechanisms.

(4 marks)

Continued...

QUESTION 2

a) You have been recruited by a major software company. The company's network is constantly facing different types of attacks. You found that the main cause was due to the lack of having a proper firewall at the company's network perimeter. In order to convince the top management to purchase a firewall system, list and justify FOUR (4) advantages of planting a firewall.

(4 marks)

b) With the aid of diagram and a brief explanation, differentiate between random overwriting viruses and prepending viruses.

(2 marks)

c) Your company has been victimized by a number of online attacks last year. Among all of these attacks, variations of phishing attacks were the most popular. Provide ONE (1) suggestion to protect against phishing attacks.

(2 marks)

d) You want to buy a firewall for your home network. While you have many options to choose from, a particular firewall device is mentioned to provide Port Address Translation (PAT) and Network Address Translation (NAT). Elaborate how PAT and NAT can contribute in strengthening the ability of firewall to keep your home network safe.

(2 marks)

Continued...

QUESTION 3

a) The first step when purchasing a specific category of firewall would be to comprehend the advantages and disadvantages of each category. Application Layer Gateways work on the application layer, state ONE (1) advantage and ONE (1) disadvantage of employing such firewalls.

(2 marks)

b) Stateless packet filtering and stateful packet filtering are two major packet filtering methods. Differentiate both of them and elaborate on TWO (2) limitations of stateful packet filters.

(4 marks)

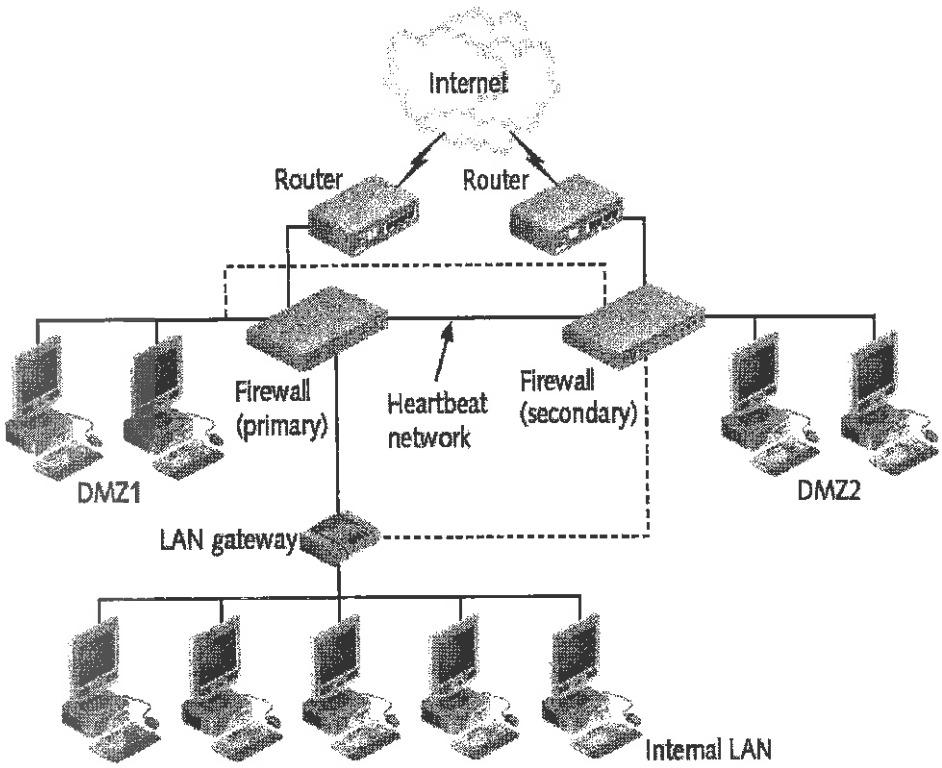
c) Bob is in charge of the network security of a medium size company (with 800 employees). In order to strengthen the security, the company installed firewalls at all endpoints of the network. Therefore, when the company's policies are changing or when a new device is added to the company's network, Bob needs to reconfigure each firewall individually. Can you think of any tool or method that can help Bob to tackle this problem? If yes, explain about the tool and elaborate on TWO (2) advantages of using such tool.

(4 marks)

Continued...

QUESTION 4

a) The figure below illustrates an example of hot standby redundancy. Why do you think it is important to have a secondary firewall as depicted in the figure? What do you think is the main role of the Heartbeat network?



(3 marks)

b) How do transparent proxies differ from non-transparent proxies? If your company wants to employ the non-transparent proxies, what would be the main advantage and disadvantage?

(4 marks)

Continued...

c) Why it is important to establish a baseline of system performance for bastion hosts?

(2 marks)

d) Why it is recommended to document any amendments are made on the bastion host's configuration?

(1 marks)

QUESTION 5

a) You company is suffering from variants of network attacks. Therefore, the managers have decided to use intrusion detection system (IDS), intrusion prevention system (IPS) and honeypots to strengthen the security of the network. Elaborate how each of the proposed measures can mitigates the risks.

(3 marks)

b) Company XYZ is planning to expand its wireless footprint by purchasing and installing a number of strong wireless antennas. Is there any security threat to this approach? Elaborate your answer.

(2 marks)

c) In your own words, differentiate between Bluesnarfing and Bluejacking.

(2 marks)

d) Explain how does a symmetric key encryption is different from an asymmetric key encryption. Provide ONE (1) secure instance for each of the encryption methods.

(3 marks)

Continued...

QUESTION 6

a) Correlation attacks and timing attacks are two types of cryptosystem's attacks. Differentiate them and suggest TWO (2) countermeasures to defend against correlation attacks.

(4 marks)

b) VPN extends network boundaries and some VPN users will have a high-speed connection that is always on. This type of users are called always-on users. However, always-on users can present the network with a set of vulnerabilities. Do you think this situation can be alleviated by providing a set of guidelines for such connections? State THREE (3) guidelines for always-on users that if followed can mitigate the vulnerabilities.

(3 marks)

c) The main goal of VPN is to provide a cost-effective and secure way to connect business locations to one another. However, adopting VPN is not completely beneficial. What do you think the THREE (3) potential drawbacks of VPN could be?

(3 marks)

End of Page